MANRS at UOG

Karl Lacanilao
Office of Information Technology

manrs.org


UNIVERSITY OF
GUAM
UNIBETSEDÅT GUÅHAN

Protect the Internet

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative that helps reduce the most common routing threats.

Join Us

MANRS History

- Published in 2014 along with website launch.
- Initial discussions date back as early as 2011 within the ISO and ITEF, and originally drafted as the "Routing Resilience Manifesto."

The MANRS Objective

Raise awareness of routing security problems and encourage the implementation of actions that can address them.

Promote a culture of collective responsibility towards the security and resilience of the Internet's global routing system.

Demonstrate the ability of the Internet industry to address routing security problems.

Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

My Experience

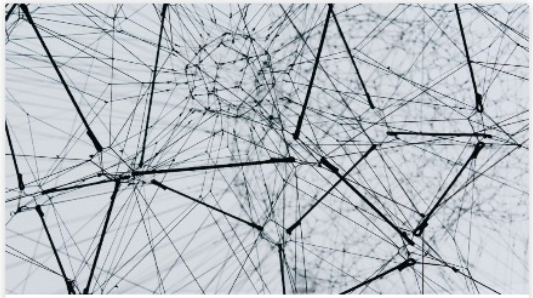
Started being network focused in 2019

Learned about BCPs and RFCs from Workshops and NOGs

First learned about MANRS in 2023

Completed application in November 2023

Different Programs



Join the Network Operators Program

Learn More →

Join the IXP Program

Learn More →

Join the CDN and Cloud Providers Program

Learn More →

Join the Equipment Vendors Program

Learn More →

https://manrs.org/join/

The MANRS Scope

Three main problems it tries to address:

1. Incorrect routing information
2. Traffic with spoofed source IP addresses
3. Coordination and collaboration between networks

Actions for Network Operators

Filtering – Prevent propagation of incorrect routing information.

Anti-spoofing – Prevent traffic with spoofed source IP addresses.

Coordination – Facilitate global operational communication and coordination between network operators.

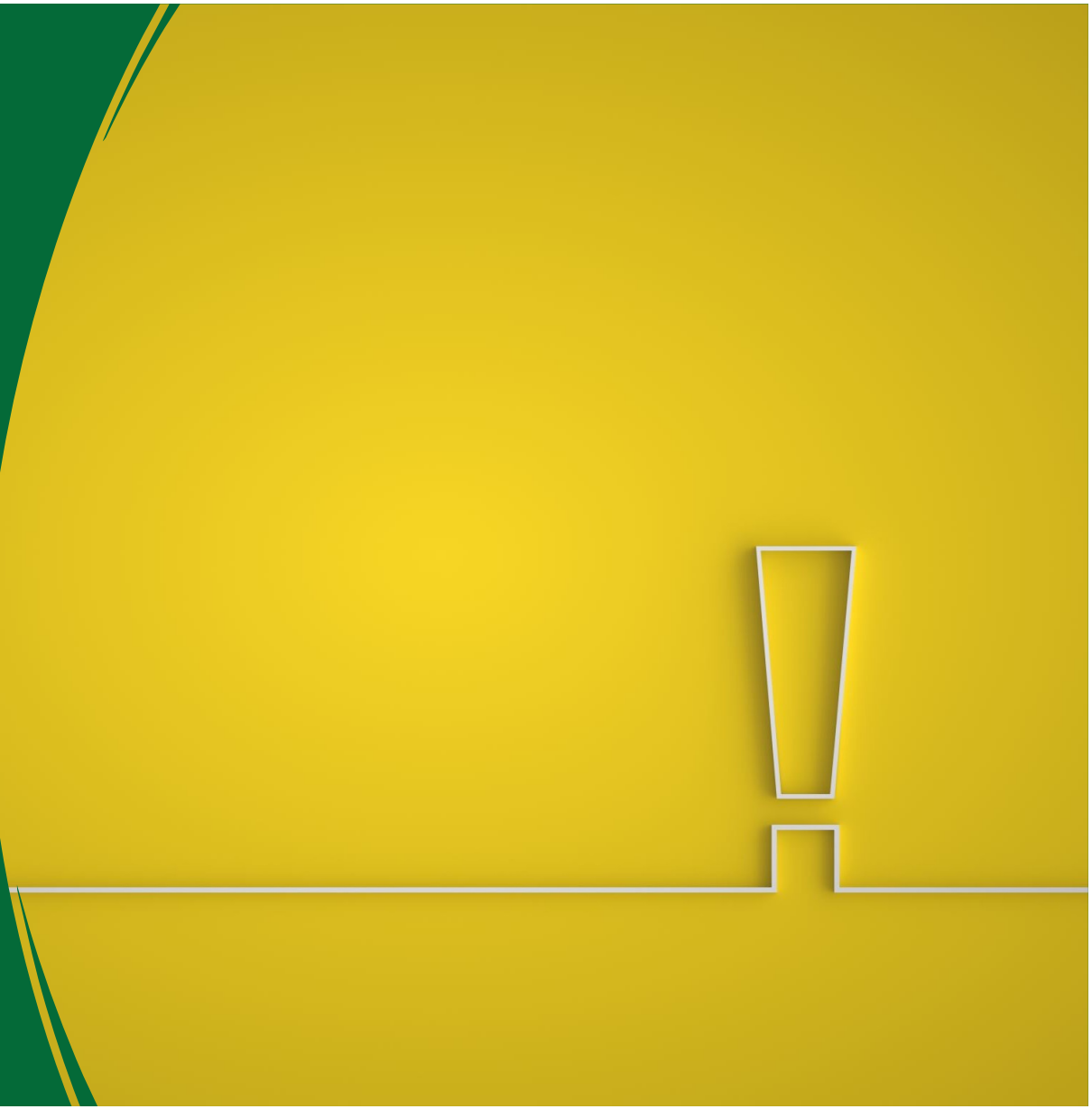
Global information – Facilitate validation of routing information on a global scale.

MANRS Action 1- Filtering

- Prevent propagation of incorrect routing information
- Filtering prefixes inbound and outbound
  - RFC8212 requires all EBGP implementations to reject prefixes received and announced in the absence of any policy
- Not recommended to set up an EBGP session without inbound and outbound prefix filters
  - If full table required, block at least the bogons

What we did for Filtering

- Configure route filters that only announce our prefixes and our downstream networks.
  - This makes us good netizens to the world.



Sample JunOS Outbound Filters

```
policy-options {
policy-statement {
UoG-IPv6-TE-out {
term UofGuam {
    from {
        family inet6;
        route-filter 2604:49c0::/32 exact;
    }
    then accept;
}
term END {
    then reject;
}
```

MANRS Action 2 - Anti-Spoofing

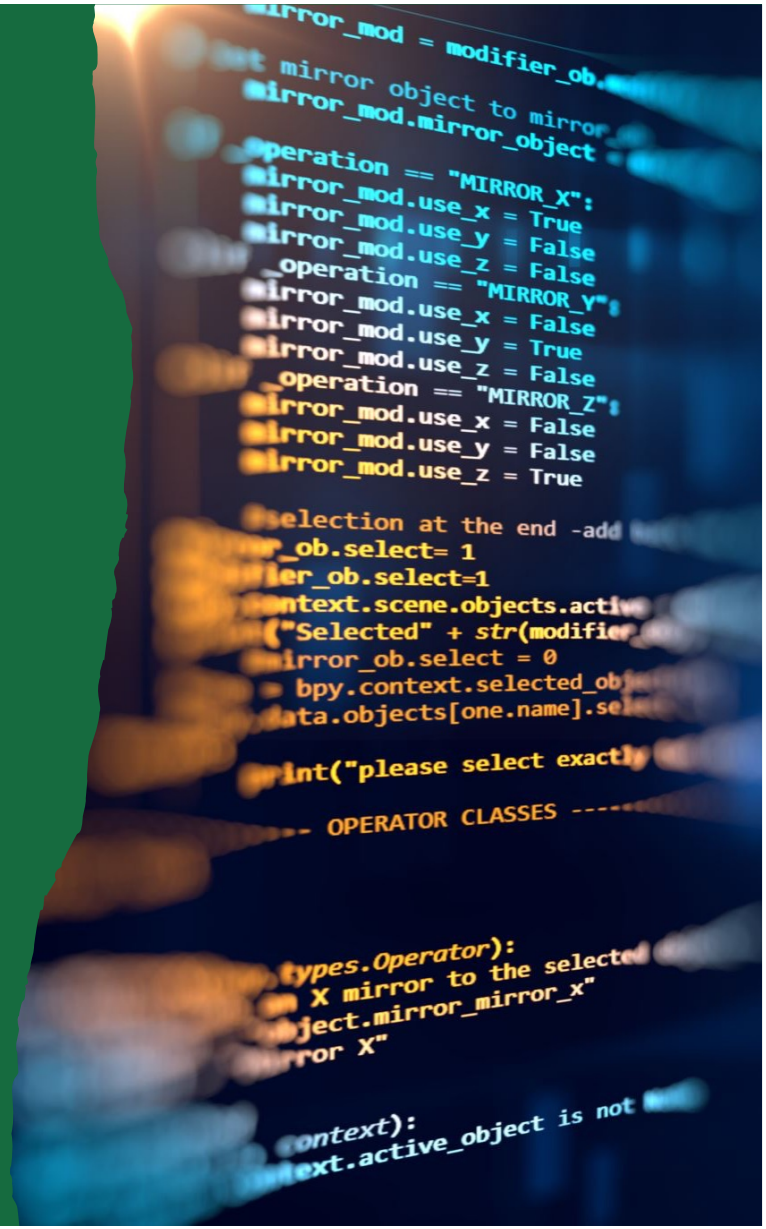
- Implementing BCP 38
  - Unicast Reverse Path Forwarding
  - (Deny outbound traffic from customers which has spoofed source addresses)

- Recommended to implement uRPF on all single-homed customer facing interfaces
  - Cheaper (CPU & RAM) than implementing packet filters

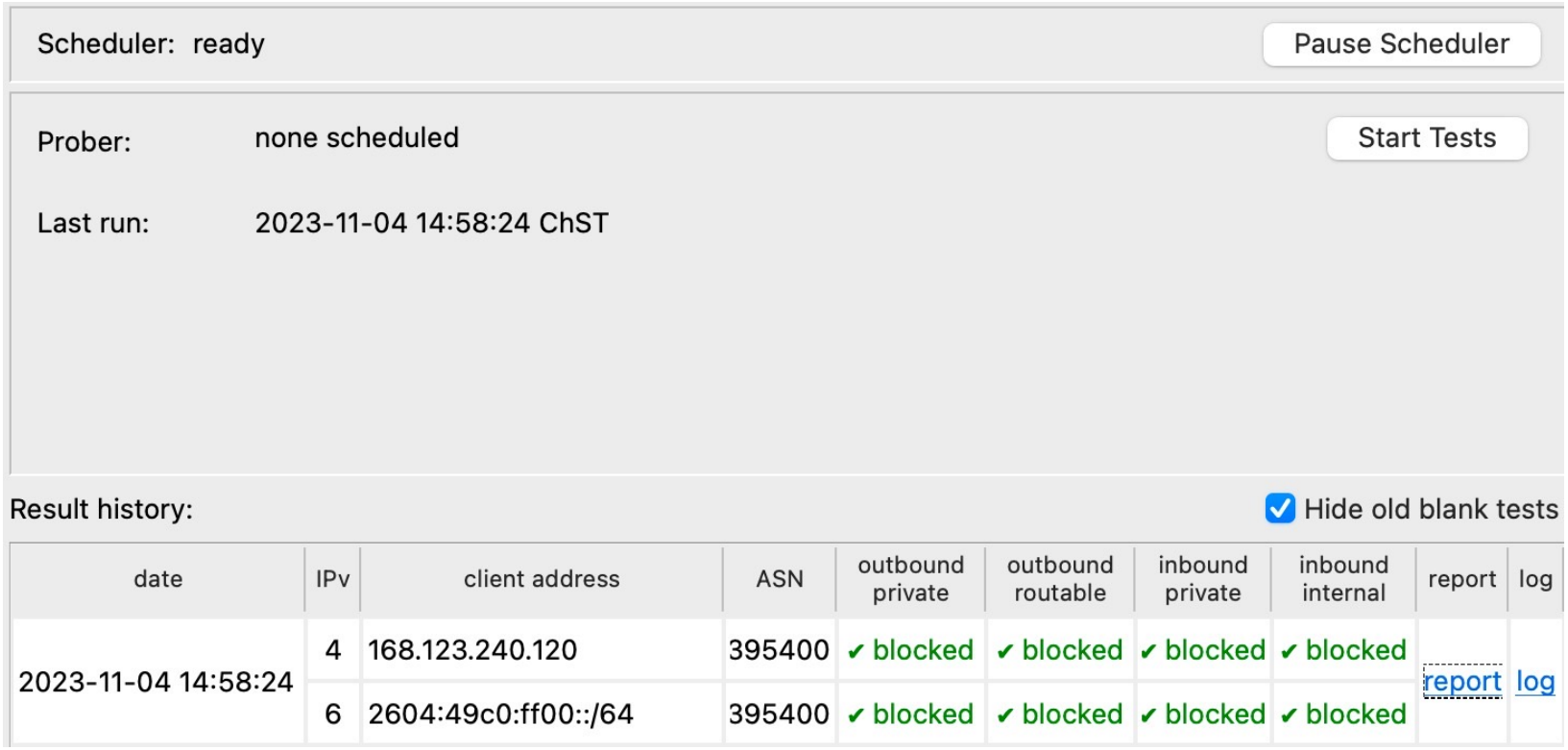
What we did for Anti-Spoofing

- We implemented uRPF on Campus VLAN Networks. We blocked incoming packets using source addresses from our address block.
- We also block bogons on the out going incase someone on campus tries to be silly.
- Tested and verified spoofing using the Caida Spoofing test program.
  - Easier to run on Mac Laptop than Windows.

https://www.caida.org/projects/spoofer/



Caida Sample Output



Scheduler: ready — Pause Scheduler

Prober: none scheduled — Start Tests

Last run: 2023-11-04 14:58:24 ChST

Result history: ☑ Hide old blank tests

date	IPv	client address	ASN	outbound private	outbound routable	inbound private	inbound internal	report	log
2023-11-04 14:58:24	4	168.123.240.120	395400	✔ blocked	✔ blocked	✔ blocked	✔ blocked	report	log
	6	2604:49c0:ff00::/64	395400	✔ blocked	✔ blocked	✔ blocked	✔ blocked		

MANRS Action 3 - Coordination

- Facilitate NOC to NOC communication
  - Know the direct NOC contacts for your customer Network Operators, your peer Network Operators, and your upstream Network Operators
  - This is not the same as calling their “customer support line”
  - Make sure NOC contact info is part of any service contract
  - Up to date info in Route and AS Objects
  - Up to date AS info in PeeringDB
- It is recommended that NOC contact info for all connected Autonomous Networks is known to your NOC

What we did for Coordination

- We made sure that our network information is accurately listed in our RIR as well other public database records like PeeringDB.
  - The ARIN RIR did make it possible to update WHOIS information for a long time, and we had to use RADB as a supplement until recently.
- All new peering sessions are accompanied with an authorized contacts list, and we also make sure it available on our website for quick lookups
- You can use free online tools like https://bgp.he.net to verify your information is accessible and verifiable by others.
  - You can also use whois tools
    - CLI # whois as#####

PeeringDB Entry & WHOIS

PeeringDB

Contact Information

Role	Name	Phone E-Mail
Abuse	UoG Network Operations Center	671-735-2640 uognoc@triton.uog.edu
Maintenance	UoG Network Operations Center	671-735-2640 uognoc@triton.uog.edu
NOC	UoG Network Operations Center	uognoc@triton.uog.edu uognoc@triton.uog.edu
Policy	UoG Network Operations Center	671-735-2640 uognoc@triton.uog.edu

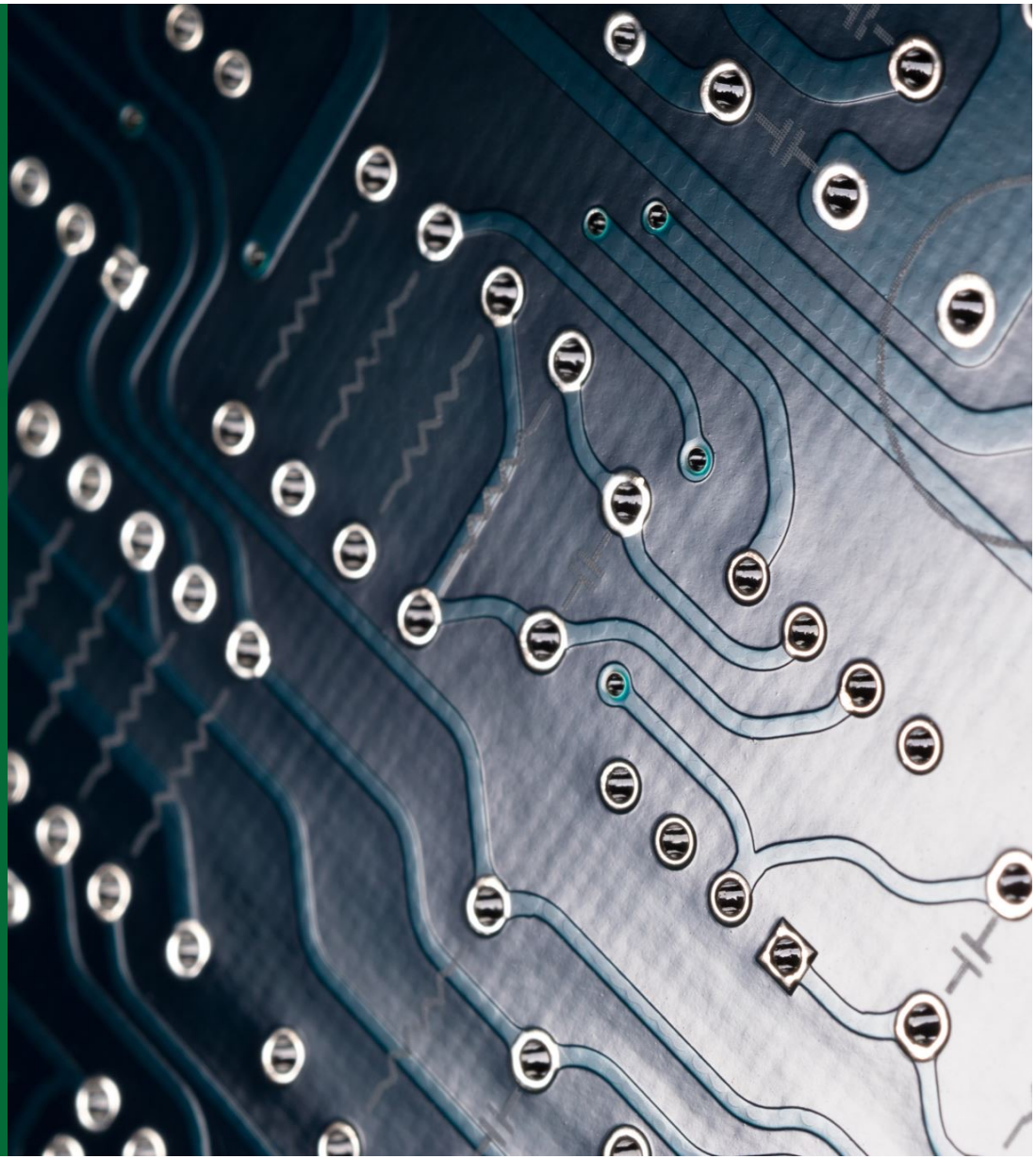
```
jdsantiago@R2D2:~$ whois as395400

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

```
OrgAbuseHandle: UOGNO-ARIN
OrgAbuseName:   UOG-NOC
OrgAbusePhone:  +16719692212
OrgAbuseEmail:  uognoc@triton.uog.edu
OrgAbuseRef:    https://rdap.arin.net/registry/entity/UOGNO-ARIN

OrgNOCHandle: UOGNO-ARIN
OrgNOCName:   UOG-NOC
OrgNOCPhone:  +16719692212
OrgNOCEmail:  uognoc@triton.uog.edu
OrgNOCRef:    https://rdap.arin.net/registry/entity/UOGNO-ARIN

RTechHandle: UOGNO-ARIN
RTechName:   UOG-NOC
RTechPhone:  +16719692212
RTechEmail:  uognoc@triton.uog.edu
RTechRef:    https://rdap.arin.net/registry/entity/UOGNO-ARIN
```

MANRS Action 4 - Global Information

- Facilitate validation of Routing Information
  - RPKI and Route Origin Authorization (ROA)
  - All routes originated need to be signed to indicate that your AS is authorized to originate these routes
    - Helps secure the global routing system

- Recommended to sign ROAs for all originated routes using RPKI
  - And make sure all customer originated routes are also signed
  - Validate received routes from all peers
    - High priority for validated routes
    - Discard invalid routes
    - Low priority for unsigned routes



What we did for Global Information

- We updated all our Routing Registry Objects and signed our ROAs
  - The University had Legacy ARIN address space that a long history in complications relative to signing ROAs
  - A recent update made it so that prior agreements regarding LRSA's would NOT be affected

- We then implemented RPKI ROV in our network to drop invalid routes as a protection against potential incoming hijacked routes.

https://manrs.org/2023/11/the-challenges-of-rpki-roa-diffusion-in-research-and-education/

Verified on RouteViews & HE's BGP tool

```
route-views>sh ip bgp 168.123.0.0/16
BGP routing table entry for 168.123.0.0/16, version 189903059
Paths: (23 available, best #7, table default)
  Not advertised to any peer
  Refresh Epoch 2
  3303 6939 395400
    217.192.89.50 from 217.192.89.50 (138.187.128.158)
      Origin IGP, localpref 100, valid, external
      Community: 3303:1006 3303:1021 3303:1030 3303:3067 6939:1000 6939:7204 6939
:8840 6939:9006
      path 7F2BF3F697C8 RPKI State valid
      rx pathid: 0, tx pathid: 0
```

Search

AS395400 UNIVERSITY OF GUAM

Quick Links
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX | Traceroute

Prefix	Description	Visibility
2604:49c0::/32	University of Guam	**100%** 69/69

Showing 1-1 of 1

RPKI ROV

2 Validator VMs

- RPKI-Client + Stay-RTR
- Routinator3000

rpki-client

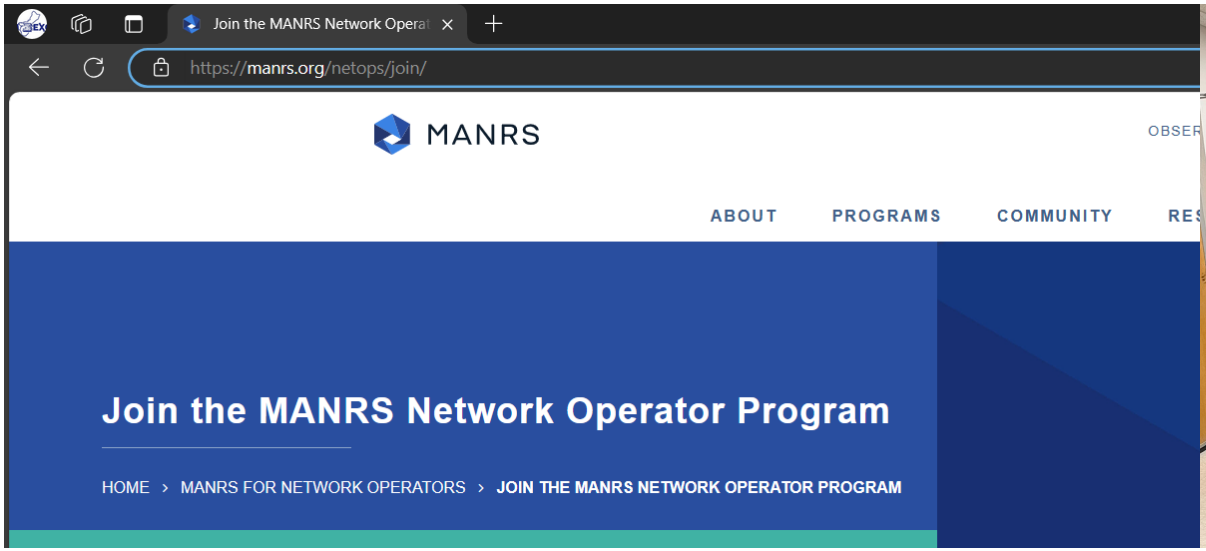
NLNETLABS

https://bgp4all.com/pfs/hints/rpki

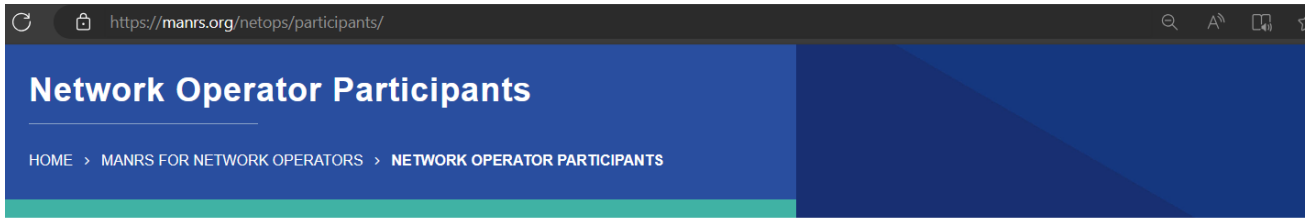
Collaboration with NSRC

In November of 2023 the NRSC came to Guam to teach a workshop and provide some Direct Engineering Assistance.

Reviewed MANRS actions and completed the application on Nov 4



Two days later.. ☺



Network operators across the globe have already committed to the MANRS initiative and implemented the Actions defined in the MANRS document.

Warning: The CSV download functionality will be deprecated on June 2024. This data can now be retrieved from the MANRS API. Read our full API documentation here.

Search Participants: guam × Show 10 entries Download CSV

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
University of Guam	6th Nov 2023	GU	395400	✓	No data	100%	100%	100%

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI

Data last measured: 1st April 2024

https://manrs.org/participant/5406/

Promote!

UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN

Admissions Academics

News & Announcements » UOG participates in a global initiative to strengthen routing security

UOG participates in a global initiative to strengthen routing security

2/15/2024

The University of Guam campus network is now a participating member of the Mutually Agreed Norms for Routing Security (MANRS) global initiative.

By participating in MANRS, UOG joins a community of security-minded organizations committed to making the global routing infrastructure more robust and secure.

Insecure routing, such as IP spoofing and network hijacking, are among the most common vectors of malicious threats to networks. Sometimes, routing errors can lead to taking entire countries and service platforms, like Google, offline.

MANRS

https://www.uog.edu/news-announcements/2024-2025/2024-uog-participates-in-a-global-initiative-to-strengthen-routing-security.php

Additional Resources

Philip Smith's BGP4All Peering toolbox

https://www.bgp4all.com/pfs/peering-toolbox

RIPE NCC MANRS Implementation Guide

https://www.ripe.net/publications/docs/ripe-706/